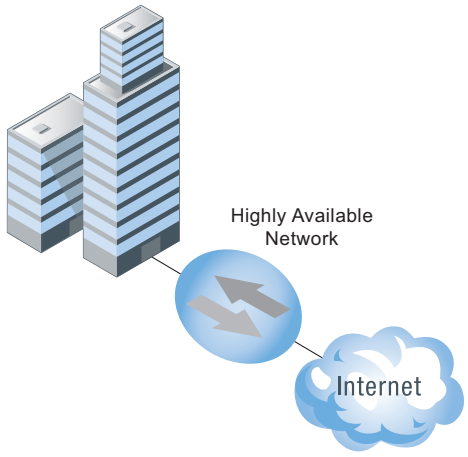
High Availability

FortiOS solves the high availability problem with our own FGCP, TCP session sync, and FRUP solutions as well as industry standard VRRP support

The Problem: Keeping Network Traffic Flowing

The basic high availability problem for TCP/IP networks and security gateways is keeping network traffic flowing. Uninterrupted traffic flow is a critical component for online systems and media access because critical business processes quickly come to a halt when the network is down. Disruptions in service are measured in dollars and cents and in loss of reputation. The competitor's site is always only a click away.

The security gateway is a crucial component of most networks since all traffic passes through it. A standalone network security gateway is a single point of failure that is vulnerable to any number of software or hardware problems that could compromise the device and bring all traffic on the network to a halt.

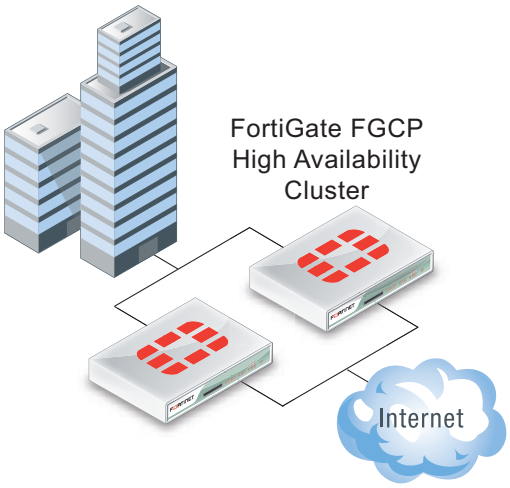


The Solution: Redundancy to Eliminate a Single Point of Failure

A common solution to the high availability problem is to eliminate the security gateway as single point of failure by introducing redundancy. With two or more redundant security gateways, if one fails, the remaining ones keep the traffic flowing. FortiOS provides four redundancy solutions: Fortinet's proprietary FGCP, FRUP, and TCP session sync solutions, and support for industry standard VRRP.

FortiGate Cluster Protocol (FGCP) HA

FortiOS FGCP HA provides cluster-based hot-standby high availability. If one of the units in an FGCP HA cluster fails, the remaining cluster units take over and network traffic continues with minimal or no interruption. FGCP HA provides stateful failover of firewall, IPsec and SSL VPN, and VoIP sessions, device failure detection and failover, and link state monitoring and failover.



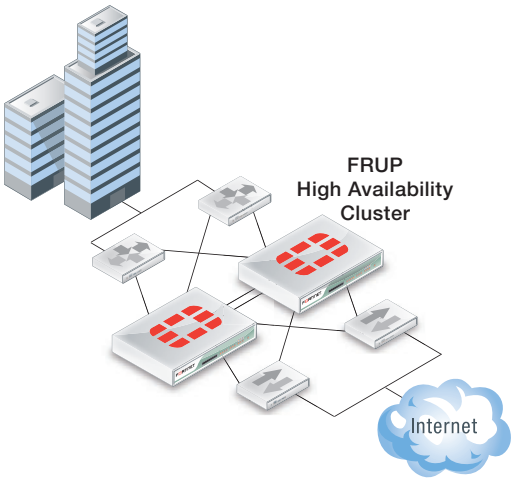
An FCGP cluster can be integrated into any TCP/IP network because the cluster appears to the network as a single FortiGate security gateway. Clusters can operate in NAT/Route or Transparent mode so they can adapt to any network environment. Active-Passive HA provides hot-standby failover protection. Active-Active HA extends the FGCP to also provide load balancing of resource-intensive TCP-based VoIP and UTM processing among all cluster units; enhancing VoIP and UTM performance.

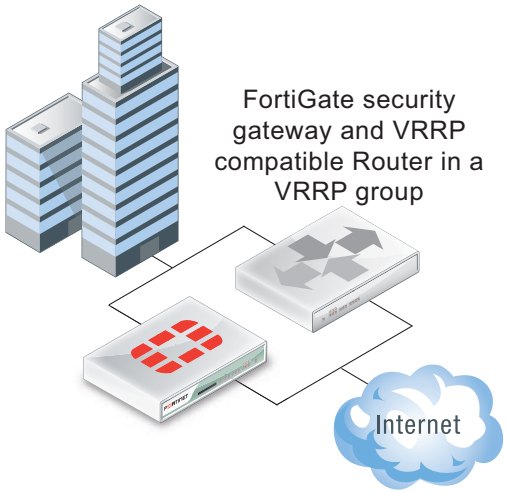
Weighted load balancing enhances active-active HA by dynamically distributing new sessions to less busy FortiGate security devices in the cluster. Fortinet accelerated network interfaces enhance FCGP load balancing and subsecond failover performance.

Fortinet Redundant UTM Protocol (FRUP)

FRUP is an extension of the FGCP that combines switching HA and firewall HA into a single unified design. A FRUP setup consists of redundant FortiGate-100D units, redundant switches, and redundant routers. In this mesh-like design the FortiGate units have redundant connections to upstream and downstream devices. The result is completely redundant connections between two networks. If any single path fails, traffic reverts to a backup path with minimal interruption.

In addition to redundancy, traffic load can be balanced between the redundant devices, leading to an overall capacity increase. The redundant devices connecting to the FortiGate units can be routers, switches, or FortiAP wireless access points.





VRRP: standards-based high availability

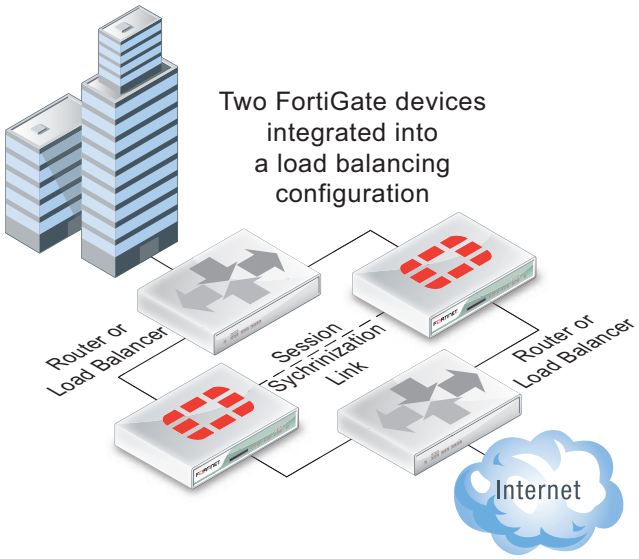
FortiGate security devices can function as master or backup Virtual Router Redundancy Protocol (VRRP) routers and can be quickly and easily integrated into a network that has already deployed VRRP. A FortiGate unit can be integrated into a VRRP group that includes any third-party VRRP devices and VRRP can provide redundancy between multiple FortiGate units.

In a VRRP configuration, when a FortiGate security device operating as the master unit fails, a backup unit takes its place and continues processing network traffic. Using VRRP virtual MAC addresses the backup unit takes over the IP address and MAC address of the failed master, reducing network disruption after the failover. If the backup unit is a FortiGate security device, the network continues to benefit from FortiGate security features. If the backup unit is a router, after a failure traffic will continue to flow, but FortiOS security features will be unavailable until the FortiGate security appliance is back on line.

FortiGate Session Life Support Protocol (FGSP)

In a network that already includes load balancing (either with load balancers or routers) for traffic redundancy, two FortiGate units can be integrated into the load balancing configuration using the FortiGate Session Life Support Protocol (FGSP). The external load balancers or routers can distribute IPv4 and IPv6 TCP, UDP, ICMP, and expectation, and NAT sessions among the FortiGate units and the FGSP performs session synchronization to keep the session tables of both FortiGate units synchronized.

If one of the FortiGate units fails, session failover occurs and active sessions fail over to the unit that is still operating. This failover occurs without any loss of data. As well, the external load balancers or routers detect the failover and re-distribute all sessions to the unit that is still operating.



The FGSP also includes configuration synchronization. Configuration changes can be made once for both FortiGate units. Settings that identify the FortiGate unit to the network, for example, interface IP addresses and BGP neighbor settings, are not synchronized so each FortiGate unit maintains its identity on the network. These settings must be configured separately for each FortiGate

Solving problems associated with redundant devices

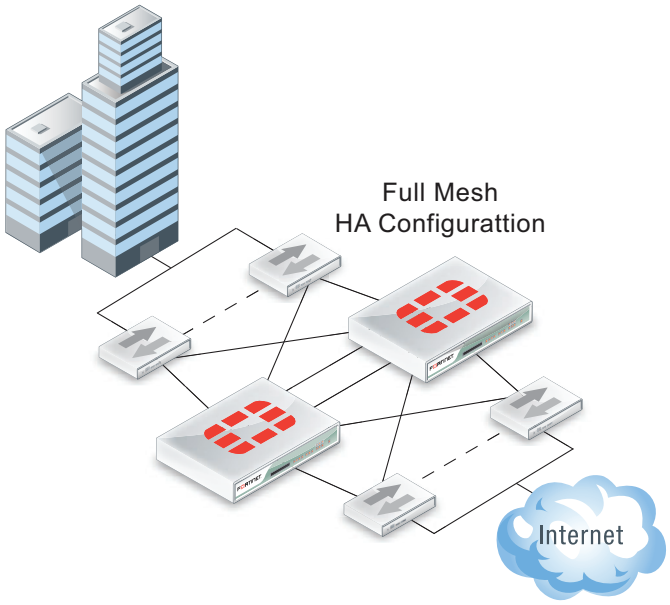
Adding more devices to a network can have its downside. More devices usually mean more management requirements. FGCP, FRUP, and TCP session sync clusters solve this problem by reducing cluster management complexity. After a few simple steps to get the cluster up and running, a cluster can be managed like a standalone FortiGate unit. Configuration changes are automatically synchronized to all cluster units. In a single step, the firmware running on all FGCP and FRUP cluster units can be upgraded or downgraded without interrupting network traffic, unlike solutions that require offline upgrades resulting in network downtime.

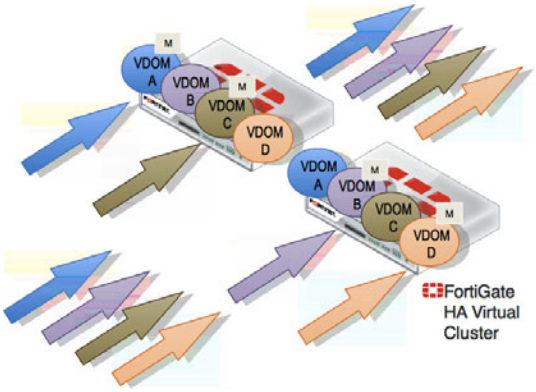
The FGCP provides IP/MAC takeover for failover protection by assigning virtual MAC addresses to the primary cluster unit and then sending gratuitous ARP packets from the primary unit interfaces after a failover to reprogram the network. Failover times can be less than a second under optimal conditions. Failover performance can be fine tuned for the network by adjusting cluster status checking, routing table updates, and failover wait timers. FGCP clusters also notify administrators of device and link failures and cluster unit status via SNMP traps, log messages, and alert email notifications. Fortinet's management and logging and reporting products, FortiManager and FortiAnalyzer, are optimized to work with FGCP HA allowing efficient and detailed cluster management.

Eliminating More Single Points of failure: Full mesh HA

A network with a redundant security gateway retains single points of failure if the redundant devices are connected to the network by standalone switches. FGCP full mesh HA removes these single points of failure by using 802.3ad aggregate or redundant interfaces on the cluster units to connect redundant switches between cluster interfaces and the network. If a redundant switch or a redundant FortiGate interface fails, network traffic can continue to flow through the still operating redundant components.

Configuring and managing a FGCP full mesh HA configuration is a simple extension to the standard aggregate/redundant interface and HA configuration and management. Using remote IP monitoring with standard or full mesh HA, clusters can also detect downstream network failures and failover to cluster units that can direct traffic around the failure.





The FCGP and VDOMs: Virtual Clustering

Virtual clustering is an extension of the FGCP for a cluster of two FortiGate units operating with multiple virtual domains (VDOMs) enabled. VDOMs create virtual machines within a FortiGate unit. Virtual clustering provides failover protection for a multiple VDOM configuration and can load balance traffic between the cluster units to improve overall network performance.

Virtual clustering load balancing efficiently load balances all traffic (including TCP and UDP traffic, UTM traffic and VoIP traffic) and can be adjusted in real time to actively optimize load sharing between the cluster units without affecting the smooth operation of the cluster.

Choosing the HA solution for your network

FortiOS solves the high availability problem with four different HA solutions. FGCP HA provides the most flexibility and the most versatility, but VRRP and TCP session synchronization and the new FRUP solution are also available to add highly available FortiGate security services to any TCP/IP network.